I/We Claim:

1. A Privacy Preserving Data-Mining Protocol, operating between a secure "aggregator" data processor and at least one of "source-entity" data processor, wherein the "aggregator" and the "source-entity" processors are interconnected via an electronic data-communications topology, and the protocol includes the steps of:

A) on the side of the "aggregator" processor: (i) from a user interface – accepting a query against a plurality of the predetermined attributes and therewith forming a parameter list, (ii) via the topology – transmitting the parameter list to each of the "source-entity" processors, (iii) via the topology – receiving a respective file from each of the "source-entity" processors, (iv) aggregating the plurality of files into a data-warehouse, (v) using the parameter list, extracting query relevant data from the data-warehouse, (vi) agglomerating the extract, and (vii) to a user interface – reporting the agglomerated extract; and

B) on the side of each processor of the at least one "source-entity" processors: (i) accumulating data-items wherein some of the data-items have privacy sensitive micro-data, (ii) organizing the data-items using the plurality of predetermined attributes, (iii) via the topology – receiving a parameter list from the "aggregator" processor, (iv) forming a file by "crunching together" the data-items according to the parameter list, (v) filtering out portions of the file which characterize details particular to less than a predetermined quantity of micro-data-specific data-items, and (vi) via the topology – transmitting the file to the "aggregator" processor.

2. The Privacy Preserving Data-Mining Protocol according to claim 1 wherein transmitting the parameter list includes transmitting a sufficiently large list of identity disclosing specifics.

3. The Privacy Preserving Data-Mining Protocol according to claim 1 wherein agglomerating the extract includes filtering out portions of the extract which characterize details particular to less than a predetermined quantity data-items.

4. The Privacy Preserving Data-Mining Protocol according to claim 3 wherein filtering out portions of the extract which characterize details particular to less than a predetermined quantity data-items includes the predetermined quantity being selected from the list, ordinal number, percentage of instances in the data-warehouse, data instances outside of mean plus predetermined number of standard distribution units.

5. The Privacy Preserving Data-Mining Protocol according to claim 1 wherein agglomerating the extract includes filtering out portions of the extract so that only identity-free micro-data remains.

6. The Privacy Preserving Data-Mining Protocol according to claim 1 wherein accepting a query includes performing a preprocessing privacy check against a predetermined source-entity data-ensemble model.

7. The Privacy Preserving Data-Mining Protocol according to claim 1 wherein "crunching together" the data-items includes joining data-items having a mutual micro-data-specific.

8. The Privacy Preserving Data-Mining Protocol according to claim 1 wherein, selected from the list of sub-steps aggregating, extracting, agglomerating, accumulating, organizing, and crunching, at least one sub-step includes fuzzy matching.

9. The Privacy Preserving Data-Mining Protocol according to claim 1 wherein filtering out portions of the file which characterize details particular to less than a predetermined quantity of micro-data-specific data-items includes selecting the predetermined quantity from the list, an ordinal number, a percentage of instances in the data-warehouse, data instances outside of statistical mean-or-median plus-and/or-minus a predetermined number of standard deviation units.

10. The Privacy Preserving Data-Mining Protocol according to claim 1 wherein accepting a query includes transforming the query into a standardized query - capable of resulting in a syndicated reporting of the agglomerated extract.

11. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for "aggregator" data processor functions in a Privacy Preserving Data-Mining Protocol, said method steps including: (i) from a user interface – accepting a query against a plurality of the predetermined attributes and therewith forming a parameter list, (ii) via an electronic data-communications topology – transmitting the parameter list to at least one "source-entity" processors, (iii) via the topology – receiving a respective file from each of the "source-entity" processors, (iv) aggregating the plurality of files into a data-warehouse, (v) using the parameter list, extracting query relevant data from the data-warehouse, (vi) agglomerating the extract, and (vii) to a user interface – reporting the agglomerated extract.

12. A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for "source-entity" data processor functions in a Privacy Preserving Data-Mining Protocol, said method steps including: (i) accumulating data-items wherein some of the data-items have privacy sensitive micro-data, (ii) organizing the data-items using the plurality of predetermined attributes, (iii) via an electronic data-communications topology – receiving a parameter list from an "aggregator" processor, (iv) forming a file by "crunching together" the data-items according to the parameter list, (v) filtering out portions of the file which characterize details particular to less than a predetermined quantity of micro-data-specific data-items, (vi) via the topology – transmitting the file to the "aggregator" processor.

13. A Privacy Preserving Data-Mining Protocol, substantially as herein before described and illustrated, firstly characterized by having at least one mutually independent "source-entity" data processors respectively forming a file by "crunching together" data-items according to a parameter list, and thereafter respectively filtering out portions of the file which characterize details particular to less than a predetermined quantity of micro-data-specific data-items; and secondly characterized by having a secure "aggregator" data processor aggregating the plurality of files into a data-warehouse.